JOURNAL OF NUMBER THEORY 27, 253–272 (1987)

Rational Points on Elliptic Curves with Complex Multiplication by the Ring of Integers in $\mathbb{Q}(\sqrt{-7})$*

J. LARRY LEHMAN

Department of Mathematics, Mary Washington College, Fredericksburg, Virginia 22401

Communicated by Hans Zassenhaus

Received June 23, 1986; revised November 18, 1986

Let E^d be the elliptic curve $y^2 = x^3 + 21dx^2 + 112d^2x$ with complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-7})$. Let ϕ be the inverse Mellin transform of $L(E^1, s)$. We construct weight $\frac{3}{2}$ cusp forms $g\theta_{28} = \sum a_n q^n$ and $h\theta_{14} = \sum b_n q^n$, which are sent to ϕ by the Shimura correspondence. We can then calculate $L(E^d, 1)$ in terms of a_d or b_d. As a consequence, the set of rational points on E^d is finite if $d \equiv 1(4)$ and $a_d \neq 0$ or if $d \equiv 2$ or $3(4)$ and $b_d \neq 0$.

INTRODUCTION

For an elliptic curve E over $\mathbb{Q}$, it is known that the set of points on E with rational coordinates, $E(\mathbb{Q})$, forms a finitely generated abelian group under a natural group law. Determination of the rank of this group for an arbitrary elliptic curve has proven to be an extremely difficult problem. A promising development in this regard is the conjecture of Birch and Swinnerton–Dyer which states in part that the rank of an elliptic curve is equal to the order of the zero of its associated L-function, $L(E, s)$, at the point $s = 1$. There has been partial confirmation of this conjecture in the case in which E has complex multiplication. In particular, a theorem of Coates and Wiles states that in this case the rank of $E(\mathbb{Q})$ is zero if $L(E, 1) \neq 0$.

In a 1983 paper [19], Tunnell applied certain results of Shimura and Waldspurger to this problem. The main result was the existence of power series (weight $\frac{3}{2}$ modular forms) whose coefficients are explicitly related to the values $L(E, 1)$ for elliptic curves E with complex multiplication by $\mathbb{Z}[i]$. Thus a sufficient condition was provided for the finiteness of $E(\mathbb{Q})$ for these curves.

* This article is a revision of the author's doctoral thesis, completed at the University of Virginia under the direction of F. Oisin McGuinness.

0022-314X/87 $3.00

641/27/3-3

In this paper, we employ Tunnell's method in the study of elliptic curves with complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-7})$. Our main result is the following.

THEOREM. *Let E^d denote the elliptic curve with equation*

$$y^2 = x^3 + 21d\,x^2 + 112d^2\,x$$

with d some positive, squarefree integer, prime to 7. There exist power series $g\theta_{28} = \sum_{n=1}^{\infty} a_n q^n$ and $h\theta_{14} = \sum_{n=1}^{\infty} b_n q^n$ (defined explicitly below) such that

(1) *if $d \equiv 1(4)$ and $a_d \neq 0$,*

(2) *if $d \equiv 2, 3(4)$ and $b_d \neq 0$,*

then the set of points on E^d with rational coefficients is finite.

1. Properties of E^d and Modular Forms

With the equation given above, E^d is an elliptic curve over $\mathbb{Q}$ for any nonzero rational number d. $E^1 = E$ is isomorphic over $\mathbb{Q}$ to the curve labeled as $49A$ in [1]. E^d is isomorphic to E over the quadratic field $\mathbb{Q}(\sqrt{d})$. We may assume that d is a squarefree integer. Let $E^d(\mathbb{Q})$ denote the group of rational points on E^d and $L(E^d, s)$ the Hasse–Weil L-series associated to E^d.

The family of curves E^d is exactly the class of elliptic curves over $\mathbb{Q}$ with complex multiplication by $\mathbb{Z}[(1+\sqrt{-7})/2]$, the ring of integers in $\mathbb{Q}(\sqrt{-7})$ [9]. The following facts are consequences of the complex multiplication of E^d.

(1) E^d is a modular curve; i.e., the inverse Mellin transform of $L(E^d, s)$ is a weight 2 cusp form which is an eigenform for all Hecke operators $T(p)$, p not dividing the conductor N_d of E^d. We denote the transform of $L(E, s)$ by ϕ. Then the cusp form associated to $L(E^d, s)$ is $\phi \otimes \chi_d$, χ_d the quadratic Dirichlet character as defined in [15]. We occasionally write $L(E^d, s)$ as $L(\phi \otimes \chi_d, s)$. The eigenvalues of ϕ under $T(p)$ for $p < 100$ are listed in [1, p. 117].

(2) There is an isogeny between E^d and E^{7d} (corresponding to a complex endomorphism in $\mathbb{Q}(\sqrt{-7})$, where E^d and E^{-7d} are the same curve). It follows that $L(E^d, s) = L(E^{-7d}, s)$ for all d.

(3) Let $\Lambda_d(s) = N_d^{s/2}(2\pi)^{-s}\,\Gamma(s)\,L(E^d, s)$. Then $\Lambda_d(s)$ is holomorphic on the entire s plane, satisfying the functional equation

$$\Lambda_d(2-s) = w_d \Lambda_d(s).$$

Furthermore, assuming 7 does not divide d, $w_d = +1$ if d is positive and

$w_d = -1$ if d is negative [8, p. 60]. Note that this means that $L(E^d, 1) = 0$ if $d < 0$ and $7 \nmid d$.

From these facts it follows that it will suffice to consider $L(E^d, 1)$ only for d positive, squarefree, and prime to 7. We claim that these values can be calculated explicitly in terms of the coefficients of certain weight $\frac{3}{2}$ cusp forms.

Let $M_k(N, \chi)$ denote the vector space of modular forms of weight $k \in \frac{1}{2}\mathbb{Z}$, level N, and character χ. Let $S_k(N, \chi)$ denote the corresponding subspace of cusp forms. A modular form $f(z)$ can be identified with its "q-expansion," i.e., its expansion as $f(z) = \sum_{n=0}^{\infty} a_n q^n$ with $q = e^{2\pi i z}$. (See [10] for definitions and details.)

Associated to the space of modular forms is the commutative algebra of Hecke operators. These are linear operators from $M_k(N, \chi)$ into itself, also preserving the subspace $S_k(N, \chi)$. If k is an integer, then this algebra is generated by all $T(p)$, p a prime number. If k is half-integral, the algebra is generated by all $T(p^2)$. By way of definition in this case, we note the effect of $T(p^2)$ on the q-expansion of a form f. Suppose that $f \in M_{k/2}(N, \chi)$ with k odd; let $f = \sum_{n=0}^{\infty} a_n q^n$ and define $\lambda = (k-1)/2$. Then $T(p^2) f = \sum_{n=0}^{\infty} b_n q^n$ with

$$b_n = a_{p^2 n} + \chi(p)\left(\frac{(-1)^{\lambda} n}{p}\right) p^{\lambda - 1} a_n + \chi(p^2) p^{k-2} a_{n/p^2}.$$

Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol and $a_{n/p^2} = 0$ if p^2 does not divide n.

Since the Hecke operators commute with one another, it follows that the spaces $M_k(N, \chi)$ and $S_k(N, \chi)$ have bases of forms which are simultaneously eigenforms of all $T(p)$ ($T(p^2)$ if $k \notin \mathbb{Z}$) if $p \nmid N$. We note here a fact which will be useful in constructing such a basis.

PROPOSITION 1. *Suppose that $S_{k/2}(N, \chi)$ has a basis of forms, $f_1, \ldots, f_n$, which are eigenforms of $T(q^2)$ for a specific prime q. Suppose that $T(q^2) f_i = \alpha f_i$ for $i = 1, \ldots, m$, some m, and that $T(q^2) f_i = \beta_i f_i$ for $i = m+1, \ldots, n$ with $\beta_i \neq \alpha$ for all such i. Let S be the subspace spanned by $f_1, \ldots, f_m$. Then $f \in S$ implies that $T(p^2) f \in S$ for all primes p.*

Remarks. The proof of this proposition is a straightforward consequence of the commutativity and linearity of the Hecke operators. This fact also holds for the entire space of modular forms, and in the case of integral weight forms (with $T(p)$ in place of $T(p^2)$).

The following theorem defines the Shimura correspondence, a map relating certain half-integral weight cusp forms to modular forms of even weight.

THEOREM [16, p. 458; 10, p. 212]. *Let $k \geq 3$ be an odd integer, N a positive*

integer divisible by 4, *and* χ *a character modulo* N. *Suppose that* $f \in S_{k/2}(N, \chi)$ *is an eigenform for all* $T(p^2)$ *with corresponding eigenvalues* λ_p. *Define a function* $g(z) = \sum b_n q^n$ *by the identity*

$$\sum_{n=1}^{\infty} b_n n^{-s} = \prod_p [1 - \lambda_p p^{-s} + \chi(p)^2 p^{k-2-2s}]^{-1}.$$

Then $g \in M_{k-1}(N/2, \chi^2)$. *Furthermore, as a consequence of this definition,* g *is an eigenform for all* $T(p)$, *also having the eigenvalues* λ_p.

The connection between modular forms and L-series values is provided by a theorem of Waldspurger. We state a special case of his result here.

THEOREM [20, pp. 378, 379; 19, p. 328]. *Let* Φ *be a cusp form of weight* 2, *level divisible by* 16, *and trivial character which is the image of a form* f *of weight* $\frac{3}{2}$ *and quadratic character* χ *under the Shimura correspondence. Then there is a function* $A(t)$ *from squarefree integers to* $\mathbb{C}$ *such that*

(i) $A(t)^2 = L(\Phi \otimes \chi^{-1} \chi_{-t}, 1)/\pi$, *and*

(ii) *for each positive integer* N, *there is a finite set* C *of functions* $c(n)$ *such that* $\{\sum A(n^{\text{s.f.}})\, c(n)\, q^n | c(n) \in C\}$ *spans the space of forms of weight* $\frac{3}{2}$, *level* N, *and character* χ *which correspond to* Φ *by the Shimura map.*

We will apply this theorem with $\Phi = \phi \otimes \chi_2$, a form in $S_2(2^6 \cdot 7^2, \chi_1)$ (see Proposition 4 below). Our task is to find weight $\frac{3}{2}$ cusp forms which are mapped to $\phi \otimes \chi_2$ by the Shimura correspondence.

2. Construction of Weight $\frac{3}{2}$ Cusp Forms

We begin by noting three facts which will be useful in constructing new forms from existing ones [16].

PROPOSITION 2. *If* $f \in S_1(N, \chi)$ *and* $\theta \in M_{1/2}(M, \psi)$, *then* $f\theta \in S_{3/2}([M, N], \chi\psi\chi_{-1})$, $[M, N]$ *the least common multiple of* M *and* N.

PROPOSITION 3. *Suppose* $f(z) = \sum a_n q^n$ *is in the space* $S_{k/2}(N, \chi)$ *with* k *odd, and let* m *be any positive integer. Then* $f(mz) = \sum a_n q^{mn} \in S_{k/2}(mN, \chi\chi_n)$.

PROPOSITION 4. *Suppose that* $f(z) = \sum a_n q^n \in S_k(N, \chi)$ *and that* s *is the conductor of* χ. *Let* ψ *be a character with conductor* r *and let* M *be the least common multiple of* N, r^2, *and* rs. *Define* $f \otimes \psi(z)$ *to be* $\sum a_n \psi(n) q^n$. *Then* $f \otimes \psi \in S_k(M, \psi^2\chi)$.

In constructing weight $\frac{3}{2}$ forms, we use two methods. The first, following Tunnell, is to construct weight 1 cusp forms by representation theory, and

then to multiply these by theta series. The second, following Shimura, is to use ternary quadratic forms to construct weight $\frac{3}{2}$ forms directly. The former method is somewhat preferable for computational purposes, while the latter is more useful in constructing an entire space of forms. In either case, finding those forms mapped to $\phi \otimes \chi_2$ by the Shimura correspondence is essentially a trial-and-error process. (See [12] for more details.)

Let formal power series be defined as

$$g_1 = \sum [q^{(14m+1)^2+(14n)^2} - q^{(14m+7)^2+(14n+6)^2}]$$

$$g_2 = \sum [q^{(14m+3)^2+(14n)^2} - q^{(14m+7)^2+(14n+4)^2}]$$

$$g_3 = \sum [q^{(14m+5)^2+(14n)^2} - q^{(14m+7)^2+(14n+2)^2}]$$

$$g_4 = \sum [q^{(14m+1)^2+(14n+2)^2} - q^{(14m+5)^2+(14n+6)^2}]$$

$$g_5 = \sum [q^{(14m+3)^2+(14n+6)^2} - q^{(14m+1)^2+(14n+4)^2}]$$

$$g_6 = \sum [q^{(14m+5)^2+(14n+4)^2} - q^{(14m+3)^2+(14n+2)^2}],$$

all sums being taken over all $m, n \in \mathbb{Z}$. Let $g' = g_1 + g_2 + g_3$, $g'' = g_4 + g_5 + g_6$, and $g = g' + g''$.

Similarly define

$$h_1 = \sum [q^{(7m+1)^2+2(7n)^2} - q^{(7m)^2+2(7n+2)^2}]$$

$$h_2 = \sum [q^{(7m+3)^2+2(7n)^2} - q^{(7m)^2+2(7n+1)^2}]$$

$$h_3 = \sum [q^{(7m+1)^2+2(7n+1)^2} - q^{(7m+3)^2+2(7n+2)^2}]$$

$$h_4 = \sum [q^{(7m+2)^2+2(7n)^2} - q^{(7m)^2+2(7n+3)^2}]$$

$$h_5 = \sum [q^{(7m+2)^2+2(7n+2)^2} - q^{(7m+1)^2+2(7n+3)^2}]$$

$$h_6 = \sum [q^{(7m+3)^2+2(7n+3)^2} - q^{(7m+2)^2+2(7n+1)^2}].$$

Let $h' = h_1 + h_2 + h_4$, $h'' = h_3 + h_5 + h_6$, and $h = h' + h''$.

PROPOSITION 5. *g', g'', and g are in $S_1(784, \chi_{-1})$, h', h'', and h are in $S_1(392, \chi_{-2})$.*

Proof. Let $f_1 = g' + \sqrt{2}\, g'' = \sum_{n=1}^{\infty} a_n q^n$ and $f_2 = g' - \sqrt{2}\, g'' = \sum_{n=1}^{\infty} b_n q^n$. Then $\sum_{n=1}^{\infty} a_n n^{-s} = L(s, \psi_1)$ and $\sum_{n=1}^{\infty} b_n n^{-s} = L(s, \psi_3)$, where ψ_1 and ψ_3 are characters on the generalized ideal class group $I(c)/P_c$ for $k = \mathbb{Q}(\sqrt{-1})$ and $c = (1+i)^2(7)$. These characters are determined by their action on a generator, such as the class of the ideal $(1+2i)$, for $I(c)/P_c$: $\psi_1(1+2i) = \zeta = e^{\pi i/4}$ and $\psi_3(1+2i) = \zeta^3$. That f_1 and f_2 are in $S_1(784, \chi_{-1})$ now follows from the Weil–Langlands theorem [7, p. 206; see also 3, pp. 70–73]. Since $S_1(784, \chi_{-1})$ is a complex vector space, the forms g', g'', and g are in $S_1(784, \chi_{-1})$ also.

The argument for h', h'', and h is exactly the same, except that $k = \mathbb{Q}(\sqrt{-2})$, $c = (7)$, and the generator of $I(c)/P_c$ which we use is $(1+\sqrt{-2})$. We omit all other details here, as we will see an alternative way of defining these forms below. ∎

Now define the theta series $\theta_t \in M_{1/2}(4t, \chi_t)$ by the power series expansion $\theta_t = \sum_{n \in \mathbb{Z}} q^{tn^2}$ [15, p. 32]. By Proposition 2, we obtain the weight $\frac{3}{2}$ cusp forms: $g\theta_7$ and $g\theta_{28} \in S_{3/2}(784, \chi_7)$, $h\theta_{14} \in S_{3/2}(392, \chi_7)$, and $h\theta_7 \in S_{3/2}(392, \chi_{14})$. We note a fact which will be useful below.

PROPOSITION 6. *If $h\theta_{14} = \sum b_n q^n$ and $h\theta_7 = \sum c_n q^n$, then $c_n = -b_{2n}$ for all n.*

The proof of this claim depends on a comparison of the representations of n and $2n$ as sums of the form $r^2 + 2s^2$ with $r, s \in \mathbb{Z}$. One can show that if $h = \sum a_n q^n$, then $a_n = -a_{2n}$ for all n from which our result follows.

We claim that the coefficients of the forms $g\theta_{28}$ and $h\theta_{14}$ suffice to describe the L-series values of the curves E^d. To see this we must consider the action of the Shimura correspondence on these forms. But to apply Shimura's theorem, we must first show that these forms are eigenforms under all Hecke operators $T(p^2)$. We first investigate the space $S_{3/2}(784, \chi_7)$ in more detail.

We consider now a general method of constructing modular forms (see [16] for details). Suppose that $f(x_1, ..., x_n)$ is a positive definite, integral quadratic form. Associate with f the matrix $A = [\partial^2 f/\partial x_i \partial x_j]$, so that $f(x_1, ..., x_n) = \frac{1}{2}\, {}^tXAX$, where ${}^tX = [x_1, ..., x_n]$. Let $D = \det A$ and let N be the smallest positive integer so that NA^{-1} has integral entries, and even diagonal entries. Define $\theta(f)$ to be the power series

$$\theta(f) = \sum q^{f(m_1, ..., m_n)},$$

where the sum is taken over all n-tuples, $(m_1, ..., m_n) \in \mathbb{Z}^n$.

PROPOSITION 7 [16, p. 456]. *$\theta(f)$ is a modular form of weight $n/2$ and level N. Its character is χ_{2D} if n is odd, χ_{-D} if $n \equiv 2(4)$, and χ_D if $n \equiv 0(4)$.*

Suppose now that two integral quadratic forms f_1 and f_2 are in the same genus, i.e., that f_1 and f_2 are equivalent in the ring of p-adic integers for each prime p, and are also equivalent in the field of real numbers. In this case we write $f_1 \vee f_2$ and also say that f_1 and f_2 are semi-equivalent.

PROPOSITION 8 [14, p. 286]. *If f_1 and f_2 are integral, positive definite, n-ary quadratic forms, and $f_1 \vee f_2$, then $\theta(f_1) - \theta(f_2)$ is a weight $n/2$ cusp form.*

Note. If f_1 and f_2 have associated matrices A_1 and A_2, then $f_1 \vee f_2$ implies that $\det A_1 = \det A_2$, so the character of $\theta(f_1) - \theta(f_2)$ is uniquely determined.

We now exhibit 12 forms in $S_{3/2}(784, X_7)$ constructed using ternary quadratic forms. As in [2] we use the following notation: if $f(x, y, z) = ax^2 + by^2 + cz^2 + ryz + szx + txy$, denote f by the array $\left(\begin{smallmatrix} a & b & c \\ r & s & t \end{smallmatrix}\right)$. We introduce the notation of $\theta(f_1, f_2)$ for $\frac{1}{2}(\theta(f_1) - \theta(f_2))$. In claiming that $\theta(f_1, f_2)$ is a cusp form, we are claiming that $f_1 \vee f_2$; we omit all details establishing semi-equivalence (see [2]). Finally, in asserting below the equality of certain of these examples with forms introduced above, we are invoking the principle that modular forms in the same space are equal if their q-expansions are identical for enough terms. (Otherwise their difference is a modular form with too many zeros at infinity, so it must be zero [13]. For a pair of forms in $S_{3/2}(784, \chi_7)$, it suffices to check equality of q-expansions to the term of q^{169} and this we have done in each case.)

(1) $$A = \theta\left(\begin{pmatrix} 1 & 28 & 196 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 28 & 49 \\ 0 & 0 & 0 \end{pmatrix}\right) = g'\theta_{28} \in S_{3/2}(784, \chi_7).$$

(2) $$B = \theta\left(\begin{pmatrix} 5 & 40 & 28 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 13 & 17 & 28 \\ 0 & 0 & 10 \end{pmatrix}\right) = g''\theta_{28} \in S_{3/2}(784, \chi_7).$$

(3) $$C = \theta\left(\begin{pmatrix} 1 & 7 & 196 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 7 & 49 \\ 0 & 0 & 0 \end{pmatrix}\right) = g'\theta_7 \in S_{3/2}(784, \chi_7).$$

(4) $$D = \theta\left(\begin{pmatrix} 5 & 40 & 7 \\ 0 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 13 & 17 & 7 \\ 0 & 0 & 10 \end{pmatrix}\right) = g''\theta_7 \in S_{3/2}(784, \chi_7).$$

(5) $$E = \theta\left(\begin{pmatrix} 1 & 14 & 98 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 14 & 49 \\ 0 & 0 & 0 \end{pmatrix}\right) = h'\theta_{14} \in S_{3/2}(392, \chi_7)$$
$$\subseteq S_{3/2}(784, \chi_7).$$

$$(6)\quad F=\theta\left(\begin{pmatrix}3 & 33 & 14\\ 0 & 0 & 2\end{pmatrix},\begin{pmatrix}6 & 17 & 14\\ 0 & 0 & 4\end{pmatrix}\right)=h''\theta_{14}\in S_{3/2}(392,\chi_7).$$

$$(7)\quad G=\theta\left(\begin{pmatrix}2 & 14 & 196\\ 0 & 0 & 0\end{pmatrix},\begin{pmatrix}4 & 14 & 98\\ 0 & 0 & 0\end{pmatrix}\right).$$

$G=h'\theta_7(2z)$, i.e., $h'\theta_7$ with all exponents doubled. $G\in S_{3/2}(784,\chi_7)$ as is $h'\theta_7(2z)$ by Proposition 3.

$$(8)\quad H=\theta\left(\begin{pmatrix}6 & 66 & 14\\ 0 & 0 & 4\end{pmatrix},\begin{pmatrix}12 & 34 & 14\\ 0 & 0 & 8\end{pmatrix}\right)=h''\theta_7(2z)\in S_{3/2}(784,\chi_7).$$

$$(9)\quad I=\theta\left(\begin{pmatrix}1 & 14 & 28\\ 14 & 0 & 0\end{pmatrix},\begin{pmatrix}2 & 4 & 49\\ 0 & 0 & 2\end{pmatrix}\right)\in S_{3/2}(196,\chi_7)$$

$$\subseteq S_{3/2}(784,\chi_7).$$

$$(10)\quad J=\frac{1}{2}\theta\left(\begin{pmatrix}3 & 3 & 10\\ -1 & 1 & 1\end{pmatrix},\begin{pmatrix}5 & 5 & 5\\ 3 & 4 & 4\end{pmatrix}\right)\in S_{3/2}(196,\chi_7).$$

$$(11)\quad K=\theta\left(\begin{pmatrix}4 & 56 & 112\\ 56 & 0 & 0\end{pmatrix},\begin{pmatrix}8 & 16 & 196\\ 0 & 0 & 8\end{pmatrix}\right)\in S_{3/2}(784,\chi_7).$$

$$(12)\quad L=\theta\left(\begin{pmatrix}6 & 14 & 20\\ 14 & 2 & 0\end{pmatrix},\begin{pmatrix}12 & 12 & 12\\ 4 & 4 & 10\end{pmatrix}\right)\in S_{3/2}(784,\chi_7).$$

THEOREM 1. *The forms A through L as defined above are eigenforms of all Hecke operators $T(p^2)$, $p\neq 2$. The eigenvalues of each are the same as the eigenvalues of ϕ under the operators $T(p)$.*

Remarks. We shall see below that these forms have no terms with exponent divisible by 7, so $T(7^2)$ applied to any of them yields 0. Thus these 12 forms are trivially eigenforms of $T(7^2)$. The dimension of the space $S_{3/2}(784,\chi_7)$ is 34 [6], greatly complicating the proof of Theorem 1. We will divide the argument into several lemmas. The most important step is the construction of a basis for $S_{3/2}(196,\chi_7)$, a subspace of $S_{3/2}(784,\chi_7)$ of dimension nine, where the effect of the Hecke operators can be fully described.

First we exhibit a basis for the space spanned by A through L made up of forms with restrictions on the exponents of the terms with nonzero coefficients. Let $r_1,\ldots,r_m$ be integers so that $0\leqslant r_i\leqslant 7$ and let s be $+1$ or -1. If $f=\sum a_n q^n$ is a modular form, we write $f\in(r_1,\ldots,r_m;s)$ to mean that $a_n=0$ unless $n\equiv r_i(8)$ for some $1\leqslant i\leqslant m$, and $(n/7)=s$.

LEMMA 1. *The forms A' through L' defined below have restrictions on nonzero coefficients as noted*:

$$A' = 2A - C + \tfrac{1}{2}E - \tfrac{1}{2}I - K = q + q^9 + q^{25} - 2q^{65} + \cdots \in (1; +1)$$

$$B' = G + K = q^2 - q^{18} + 2q^{22} - 2q^{30} + 2q^{46} - q^{50} + 2q^{58} + \cdots \in (2, 6; +1)$$

$$C' = \tfrac{1}{2}(D + F + H + J + L) = q^3 - q^{19} - 2q^{31} + 2q^{55} + q^{59} + \cdots \in (3, 7; -1)$$

$$D' = -\tfrac{1}{2}A + \tfrac{1}{2}C + K = q^4 - 2q^{32} + q^{36} - 2q^{64} + \cdots \in (0, 4; +1)$$

$$E' = \tfrac{1}{2}(2B - D + F + H - J - L) = q^5 - q^{13} - q^{45} - q^{61} + \cdots \in (5; -1)$$

$$F' = -B + D + \tfrac{1}{2}H + \tfrac{1}{2}L = q^6 - 2q^{26} - q^{34} + q^{38} + \cdots \in (2, 6; -1)$$

$$G' = \tfrac{1}{2}(-A + C) = q^8 + q^{16} + q^{32} - 2q^{60} + q^{64} + \cdots \in (0, 4; +1)$$

$$H' = \tfrac{1}{2}(-B + D) = q^{12} - q^{20} - q^{24} + q^{48} + q^{52} + \cdots \in (0, 4; -1)$$

$$I' = \tfrac{1}{4}(-4A + 2C + E + 2G + I + 2K)$$
$$= q^{15} + q^{23} + q^{39} - q^{51} - q^{67} + \cdots \in (3, 7; +1)$$

$$J' = \tfrac{1}{2}(-D + F + H - J - L) = q^{17} - 2q^{23} + q^{41} + \cdots \in (1; -1)$$

$$K' = \tfrac{1}{2}(B - D + H - L) = q^{20} - 2q^{48} - q^{52} - q^{68} + \cdots \in (0, 4; -1)$$

$$L' = \tfrac{1}{4}(-2A + 2C - E + I + 2K) = q^{29} + q^{37} + \cdots \in (5; +1).$$

We omit the proof of this lemma, which depends on a case by case comparision of the definitions of the forms A through L, establishing correspondences between solutions of quadratic forms. Note that multiplication of n by p^2 leaves fixed the congruence class of n modulo 8 (if $p \neq 2$) and the Legendre symbol $(n/7)$ (if $p \neq 7$). Thus recalling the definition of $T(p^2)$ above, it follows that $f \in (r_1, ..., r_m; s)$ implies that $T(p^2)f \in (r_1, ..., r_m; s)$ also, if $p \neq 2, 7$.

Now we turn our attention to the space $S_{3/2}(196, \chi_7)$. I and J are in this space as are the forms

(1) $$P = \theta\left(\begin{pmatrix} 1 & 1 & 7 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 4 \\ 2 & 0 & 0 \end{pmatrix}\right) \in S_{3/2}(28, \chi_7) \subseteq S_{3/2}(196, \chi_7).$$

(2) $$Q = \theta\left(\begin{pmatrix} 7 & 49 & 49 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 14 & 28 & 49 \\ 0 & 0 & 14 \end{pmatrix}\right) \in S_{3/2}(196, \chi_7).$$

(3) $$R = \theta\left(\begin{pmatrix} 1 & 7 & 49 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 7 & 2 & 25 \\ 2 & 0 & 0 \end{pmatrix}\right) \in S_{3/2}(196, \chi_7).$$

(4) $$S = \theta\left(\begin{pmatrix} 1 & 7 & 49 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 & 49 \\ 0 & 0 & 2 \end{pmatrix}\right) \in S_{3/2}(196, \chi_7).$$

(5) $T=\frac{1}{2}\theta\left(\begin{pmatrix}1 & 2 & 49\\ 0 & 0 & 1\end{pmatrix},\begin{pmatrix}1 & 7 & 14\\ 7 & 0 & 0\end{pmatrix}\right)\in S_{3/2}(196,\chi_7)$.

(6) Consider the form K' above. By Lemma 1, K' only has terms with exponent divisible by 4. Thus K' is of the form $f(4z)$ for some $f\in S_{3/2}(196,\chi_7)$. Denote this form by U.

(7) $V=\frac{1}{2}\sum_{m\in\mathbb{Z}}\chi_{-7}(m)\,mq^{m^2}$. $V\in S_{3/2}(196,\chi_7)$ [16, p. 457].

LEMMA 2. *The forms I, J, P, Q, R, S, T, U, and V make up a basis for the space $S_{3/2}(196,\chi_7)$.*

Now for $f\in S_{3/2}(196,\chi_7)$, it is possible to write $T(p^2)f$ explicitly as a sum of the basis forms. Let $R'=3R-2V$ and $S'=4S-3R-2I+2V$. Then the following lemma is verified by direct computation.

LEMMA 3. *The forms I, J, P, Q, R', S', T, U, and V form a basis of $S_{3/2}(196,\chi_7)$ made up of eigenforms of $T(3^2)$. I, J, T, and U have eigenvalue 0, P, Q, and S' have eigenvalue -2, R' has eigenvalue 2, and V has eigenvalue 4.*

Now applying Proposition 1, the subspace spanned by I, J, T, and U is invariant under all $T(p^2)$. Let

$$W=I+T=q-2q^8+q^9-2q^{16}+q^{25}+2q^{29}+\cdots$$
$$X=T=q^2+q^4+q^8-2q^{15}+q^{16}-q^{18}+2q^{22}-2q^{23}-2q^{29}+\cdots$$
$$Y=J+U=q^3-q^6-q^{12}-q^{17}-q^{19}+2q^{20}+q^{24}+2q^{26}+\cdots$$
$$Z=U=q^5-2q^{12}-q^{13}-q^{17}+2q^{20}+2q^{24}+\cdots.$$

It can be checked (by comparing enough coefficients, since $S_{3/2}(196,\chi_7)\subseteq S_{3/2}(784,\chi_7)$) that $W=A'-2G'+2L'$, $X=B'+D'+G'-2I'-2L'$, $Y=C'-F'-H'-J'+K'$, and $Z=E'-2H'-J'$.

LEMMA 4. *W, X, Y, and Z are eigenforms of all $T(p^2)$, $p\neq 2, 7$. Their eigenvalues are those of ϕ under $T(p)$.*

Proof. Let p be a prime other than 2 or 7. Then

$$T(p^2)\,W=\alpha W+\beta X+\gamma Y+\delta Z$$

for some α, β, γ, and δ depending on p. But since $W=A'-2G'+2L'\in(0, 1, 4, 5; +1)$ in the above notation, $T(p^2)\,W\in(0, 1, 4, 5; +1)$ as well. So for instance if $T(p^2)\,W=\sum a_n q^n$, then a_2, a_3, and a_5 are all zero. But on the right-hand side of the above equation, the coefficients of q^2, q^3, and q^5

are respectively β, γ, and δ. Thus $T(p^2)\, W = \alpha W$ for some α depending on p; that is, W is an eigenform of $T(p^2)$ for $p \neq 2, 7$. Similar arguments show that X, Y, and Z are all eigenforms of the same Hecke operators.

That these forms have the same eigenvalues under $T(p^2)$ as ϕ has under $T(p)$ can be checked directly for $p < 100$. Since under the Shimura correspondence, the image of these forms must be some weight 2 form of level dividing 98, it is clear by checking Table 3 in [1] that these forms must have all eigenvalues in common with ϕ. ∎

LEMMA 5. *The forms A' through L' are all eigenforms of all $T(p^2)$, $p \neq 2, 7$. Each has the same eigenvalues as does ϕ.*

Proof. Let $A' = \sum a_n q^n$ and $T(p^2)\, A' = \sum b_n q^n$ for some $p \neq 2, 7$. Since $T(p^2)\, W = \lambda_p W$ for some value λ_p, we have that

$$T(p^2)(A' - 2G' + 2L') = \lambda_p(A' - 2G' + 2L'),$$

i.e.,

$$T(p^2)\, A' - 2T(p^2)\, G' + 2T(p^2)\, L' = \lambda_p A' - 2\lambda_p G' + 2\lambda_p L'.$$

If $n \equiv 1(8)$ and $(n/7) = 1$, the coefficient of q^n on the left-hand side is b_n and that on the right-hand side is $\lambda_p a_n$. On the other hand, if n is any other positive integer, then we have seen that $a_n = 0 = b_n$. So $b_n = \lambda_p a_n$ for all n and $T(p^2)\, A' = \lambda_p A'$. Similar arguments establish that the other forms are also eigenforms of $T(p^2)$ for $p \neq 2, 7$, each having the same eigenvalues as do W, X, Y, and Z, i.e., those of ϕ. ∎

Since each form A' through L' has the same eigenvalue under $T(p^2)$, the linear combinations A through L are also eigenforms with the same eigenvalue. Thus Theorem 1 is proved.

In particular, if $T(p)\, \phi = \lambda_p \phi$, then $T(p^2)\, g\theta_{28} = \lambda_p\, g\theta_{28}$ and $T(p^2)\, h\theta_{14} = \lambda_p\, h\theta_{14}$, if p is any prime other than 2. Using Proposition 6, one can also show directly that $T(p^2)\, h\theta_7 = \lambda_p\, h\theta_7$ for $p \neq 2$.

Now define $\sqrt{\chi_2}$ to be the Dirichlet character of conductor 16 which is determined by $\sqrt{\chi_2}\,(3) = i = \sqrt{\chi_2}\,(5)$. Note that $[\sqrt{\chi_2}\,(n)]^2 = \chi_2(n)$ for all n. Let f be any one of $g\theta_{28}$, $h\theta_{14}$, or $h\theta_7$. Again, it can be shown directly that

$$T(p)(\phi \otimes \chi_2) = \lambda_p \chi_2(p)(\phi \otimes \chi_2)$$

and that

$$T(p^2)(f \otimes \sqrt{\chi_2}) = \lambda_p \chi_2(p)(f \otimes \sqrt{\chi_2})$$

for $p \neq 2$ [12]. But now it is trivially the case that

$$T(2)(\phi \otimes \chi_2) = 0 = T(2^2)(f \otimes \sqrt{\chi_2}).$$

Thus we have the following:

COROLLARY 1. *The weight 2 cusp form $\phi \otimes \chi_2$ is the image under the Shimura correspondence of each of the weight $\frac{3}{2}$ forms $g\theta_{28} \otimes \sqrt{\chi_2}$, $h\theta_{14} \otimes \sqrt{\chi_2}$, and $h\theta_7 \otimes \sqrt{\chi_2}$.*

3. CALCULATION OF L-SERIES VALUES

We now fix the following notation: let $g\theta_{28} = \sum a_n q^n$, $h\theta_{14} = \sum b_n q^n$, and $h\theta_7 = \sum c_n q^n$. We will prove that the L-series values $L(E^d, 1)$ can be expressed in terms of the coefficients of these forms.

From Proposition 4 and Corollary 1, $g\theta_{28} \otimes \sqrt{\chi_2}$ and $h\theta_{14} \otimes \sqrt{\chi_2}$ are in the subspace of $S_{3/2}(2^8 \cdot 7^2, \chi_{14})$ of forms sent to $\phi \otimes \chi_2$ by the Shimura map. Now by Waldspurger's theorem, there is a function $A_1(t)$ and a finite set of functions C such that $\{\sum A_1(n^{\text{s.f.}})\, c(n)\, q^n | c(n) \in C\}$ spans this subspace. Also we know that

$$A_1(t)^2 = \frac{1}{\pi} L(\phi \otimes \chi_2 \chi_{14}^{-1} \chi_{-t}, 1) = \frac{1}{\pi} L(\phi \otimes \chi_{-7t}, 1)$$

$$= \frac{1}{\pi} L(E^{-7t}, 1) = \frac{1}{\pi} L(E^t, 1)$$

for any squarefree t.

Furthermore, the set C is described as follows. Each function $c(n)$ in C can be expressed as $\prod_p c_p(n)$ over all places of $\mathbb{Q}$ with the following restriction of c_p to squarefree n:

$$c_\infty(n) = n^{1/4}$$

$$c_2(n) = \text{a characteristic function of } \mathbb{Q}_2^x / \mathbb{Q}_2^{x^2}$$

$$c_7(n) = \text{a characteristic function of } \mathbb{Q}_7^x / \mathbb{Q}_7^{x^2}$$

$$c_p(n) = 1 \text{ for all other } p \text{ [20, VIII.4]}.$$

Thus a basis for the subspace of $S_{3/2}(2^8 \cdot 7^2, \chi_{14})$ consisting of the forms which are sent to $\phi \otimes \chi_2$ by the Shimura correspondence is given by the eight forms $f_{a,b}$ where $a \in \{1, 3, 5, 7\}$ and $b \in \{1, -1\}$. $f_{a,b}$ is defined by

$$f_{a,b} = \sum_{n=1}^{\infty} A_1(n^{\text{s.f.}})\, c_{a,b}(n)\, q^n,$$

where for squarefree n, $c_{a,b}(n) = n^{1/4}$ if $n \equiv a(8)$ and $(n/7) = b$, and $c_{a,b} = 0$ otherwise. We do not need to describe $c_{a,b}$ on other values of n.

So there are constants $\alpha_{a,b}$ (a, b in the same sets as above) so that for instance $g\theta_{28} \otimes \sqrt{\chi_2} = \sum_{(a,b)} \alpha_{a,b} f_{a,b}$. If n is squarefree, $n \equiv a(8)$ and $(n/7) = b$, then comparing coefficients yields

$$a_n \sqrt{\chi_2}\,(n) = \alpha_{a,b}\, A_1(n) \cdot n^{1/4}.$$

So

$$a_n^2 \chi_2(n) = \alpha_{a,b}^2\, A_1(n)^2\, n^{1/2} = \alpha_{a,b}^2 \frac{1}{\pi} L(E^n, 1)\, n^{1/2}.$$

If $\alpha_{a,b} \neq 0$, then $L(E^n, 1) = (\pi\, a_n^2 \chi_2(n))/(\alpha_{a,b}^2\, n^{1/2})$.

Let Ω be the fundamental real period of the lattice by which E is defined ($\Omega = \Gamma(\frac{1}{7})\,\Gamma(\frac{2}{7})\,\Gamma(\frac{4}{7})/2\pi\sqrt{7}$ [8, p. 82]). Define Ω_n to be $\Omega/\sqrt{n}$ if $n \equiv 1(4)$ and to be $\Omega/2\sqrt{n}$ if $n \equiv 2, 3(4)$. Ω_n is the fundamental real period of E^n. In [17, p. 204] we have a table which lists, for even quadratic characters χ_n of conductor less than 500, a value $\Lambda(\chi_n) = L(\phi \otimes \chi_n, 1)/\Omega_n$. So we also have $L(E^n, 1) = \Lambda(\chi_n)\,\Omega_n$ for small n. Using this table, we can calculate $\alpha_{a,b}^2$ as $(\pi\, a_n^2 \chi_2(n))/(\Lambda(\chi_n) \cdot \Omega_n \cdot n^{1/2})$, and thus write $L(E^n, 1)$ as a specific multiple of a_n^2.

EXAMPLE. $a_5 = 1 = \Lambda(\chi_5)$, $\chi_2(5) = -1$, so $\alpha_{5,-1}^2 = -\pi/(\Omega_5 \cdot \sqrt{5}) = -\pi/\Omega$. But then for any positive, squarefree n, for which $n \equiv 5(8)$ (which means $\chi_2(n) = -1$) and $(n/7) = -1$, we have

$$L(E^n, 1) = \frac{-\pi\, a_n^2}{-\pi \cdot n^{1/2}} \cdot \Omega = a_n^2\, \Omega_n.$$

Using $g\theta_{28} \otimes \sqrt{\chi_2}$ we find similar facts for $L(E^n, 1)$ with $n \equiv 1(4)$. The constants $\alpha_{a,b} = 0$ if $a \equiv 3(4)$, but for $n \equiv 3(4)$, we find equations relating $L(E^n, 1)$ to b_n^2, using the fact that $h\theta_{14} \otimes \sqrt{\chi_2}$ is also in the space spanned by the $f_{a,b}$.

Similarly, $h\theta_7 \otimes \sqrt{\chi_2}$ is in the subspace of $S_{3/2}(2^8 \cdot 7^2, \chi_7)$ of forms sent to $\phi \otimes \chi_2$ by the Shimura map. This subspace is also spanned by eight forms (again denoted $f_{a,b}$) which are defined by

$$f_{a,b} = \sum A_2(n^{\text{s.f.}})\, c_{a,b}(n)\, q^n$$

with $c_{a,b}$ exactly as above. In this case, $A_2(t)$ has the property that

$$A_2(t)^2 = \frac{1}{\pi} L(\phi \otimes \chi_2 \chi_7^{-1} \chi_{-t}, 1) = \frac{1}{\pi} L(\phi \otimes \chi_{-14t}, 1)$$

$$= \frac{1}{\pi} L(E^{-14t}, 1) = \frac{1}{\pi} L(E^{2t}, 1).$$

$$h\theta_7 \otimes \sqrt{\chi_2} = \sum_{(a,b)} \beta_{a,b} f_{a,b}$$

for some constants $\beta_{a,b}$. If $n \equiv a(8)$, $(n/7) = b$, and n is squarefree, then

$$c_n \sqrt{\chi_2}(n) = \beta_{a,b} A_2(n) n^{1/4}$$

so $c_n^2 \chi_2(n) = \beta_{a,b}^2 A_2(n)^2 n^{1/2} = \beta_{a,b}^2 (1/\pi) L(E^{2n}, 1) n^{1/2}$. But again, for small values of n, the table in [17] gives us that

$$L(E^{2n}, 1) = \Lambda(\chi_{2n}) \Omega_{2n} = \Lambda(\chi_{2n}) \Omega / 2\sqrt{2n}.$$

Thus

$$\beta_{a,b}^2 = \frac{\pi c_n^2 \chi_2(n) \cdot 2\sqrt{2}}{\Lambda(\chi_{2n}) \Omega}.$$

EXAMPLE. $c_1^2 = 1$ and $\Lambda(X_2) = 2$ so $\beta_{1,1}^2 = (\pi \cdot 2\sqrt{2})/2\Omega = \pi\sqrt{2}/\Omega$. But then for any positive squarefree n with $n \equiv 1(8)$ and $(n/7) = 1$, we have that

$$L(E^{2n}, 1) = \frac{\pi \cdot c_n^2 \Omega}{\pi \cdot \sqrt{2} \cdot n^{1/2}} = \frac{c_n^2 \Omega}{\sqrt{2n}} = 2c_n^2 \Omega_{2n}.$$

Recalling from Proposition 6 that $c_n = -b_{2n}$ for all n, it follows that

$$L(E^{2n}, 1) = 2b_{2n}^2 \Omega_{2n}.$$

There are similar expressions for $L(E^{2n}, 1)$ in terms of b_{2n}^2 for all other n. We summarize all of these results in the following:

THEOREM 2. *Suppose that d is positive, squarefree, and prime to 7. Let $g\theta_{28} = \sum a_n q^n$ and $h\theta_{14} = \sum b_n q^n$. Then*

(1) *if* $d \equiv 1(4)$, *then* $L(E^d, 1) = \begin{cases} \frac{1}{2} \Omega_d a_d^2 & \text{if } (d/7) = 1 \\ \Omega_d a_d^2 & \text{if } (d/7) = -1 \end{cases}$

and

(2) *if* $d \equiv 2, 3(4)$, *then* $L(E^d, 1) = \begin{cases} 2\Omega_d b_d^2 & \text{if } (d/7) = 1 \\ 4\Omega_d b_d^2 & \text{if } (d/7) = -1. \end{cases}$

Remark. These results are entirely consistent with the table of adjusted L-series values in [17].

Our main result is now an immediate corollary of this theorem and the following theorem of Coates and Wiles.

THEOREM [5, p. 223]. *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by the ring of integers in a quadratic field of class number* 1. *Let r denote the rank of the group of rational points $E(\mathbb{Q})$ of E. If $r \geqslant 1$, then $L(E, 1) = 0$.*

Noting from Theorem 2 that $L(E^d, 1) = 0$ if and only if the appropriate value a_d or b_d is zero, the following result is immediate.

COROLLARY 2. *Let $d, g\theta_{28}$, and $h\theta_{14}$ be as in Theorem* 2. *Let $E^d(\mathbb{Q})$ denote the group of rational points on E^d. Then if*

$$(1) \quad d \equiv 1(4) \qquad \text{and} \qquad a_d \neq 0,$$

or

$$(2) \quad d \equiv 2, 3(4) \qquad \text{and} \qquad b_d \neq 0,$$

then $E^d(\mathbb{Q})$ is finite.

Under the conjecture of Birch and Swinnerton-Dyer, the converse of this statement is also true.

The calculations of Theorem 2 can also be applied to a second part of the Birch/Swinnerton-Dyer conjecture. Let $\mathbf{W}^d$ denote the Tate-Shafarevitch group associated to E^d over $\mathbb{Q}$. It is conjectured that if $E^d(\mathbb{Q})$ is finite, then

$$[L(E^d, 1)/\Omega_d] \cdot |E^d(\mathbb{Q})|^2 = |\mathbf{W}^d| \cdot \Pi\, c_p,$$

where $c_p = [E^d(\mathbb{Q}_p) : E_0^d(\mathbb{Q}_p)]$ is a constant depending on p and d, and the product is taken over all primes p (see [18] for details).

It is known that for all d, $|E^d(\mathbb{Q})_{\text{tors}}| = 2$, i.e., there are only two rational points on E^d of finite order, the point at infinity and $(0, 0)$. The c_p terms can be calculated using Tate's algorithm [1, pp. 46–52] as follows: If $p \nmid 14d$, then $c_p = 1$; $c_7 = 2$ for all d; $c_2 = 1$ if $d \equiv 1(4)$ and $c_2 = 4$ if $d \equiv 2, 3(4)$; and if $p \neq 2, 7$ divides d, then $c_p = 4$ if $(p/7) = 1$ and $c_p = 2$ if $(p/7) = -1$.

Given a number d as above, let l_1 be the number of odd prime divisors p of d such that $(p/7) = 1$, and let l_2 be the number of such divisors such that $(p/7) = -1$. Define l to be $l_1 + \frac{1}{2}l_2$ if l_2 is even, and to be $l_1 + \frac{1}{2}(l_2 - 1)$ if l_2 is

odd. Combining these results with the statement of Theorem 2, we make the following:

Conjecture. Let d be positive, squarefree, and prime to 7. Then

$$(1) \quad \text{if } d \equiv 1(4) \quad \text{and} \quad a_d \neq 0, \qquad \text{then} \quad |\mathbf{W}^d| = \frac{a_d^2}{4^l}$$

and

$$(2) \quad \text{if } d \equiv 2, 3(4) \quad \text{and} \quad b_d \neq 0, \qquad \text{then} \quad |\mathbf{W}^d| = \frac{b_d^2}{4^l}.$$

Note that under this conjecture $|\mathbf{W}^d|$ is a square (although it is not obvious that it is an integer). This agrees with a known property of the Tate–Shafarevitch group, that its order is a square if it is finite [4, p. 283].

We summarize the results and conjectures in the following table. To each positive integer d which is squarefree and not divisible by 7, we associate a value $s(d)$ defined by

$$s(d) = \begin{cases} a_d/2^l & \text{if } d \equiv 1(4) \\ b_d/2^l & \text{if } d \equiv 2, 3(4) \end{cases}$$

with a_d, b_d and l as above. In Table I we list the values of $s(d)$ for $d < 2000$.

In summary, if $s(d) \neq 0$, then $E^d(\mathbb{Q})$ is finite and conjecturally $s(d)^2$ is the order of the Tate–Shafarevitch group $\mathbf{W}^d$. If $s(d) = 0$, then conjecturally $E^d(\mathbb{Q})$ is infinite; i.e., there is a nontrivial rational solution to E^d.

As a partial confirmation of these conjectures, we note the following result of Rubin and Wiles.

THEOREM [11, p. 237]. *Let $s(d)$ be as above, and let $(\mathbf{W}^d)_7$ denote the kernel in $\mathbf{W}^d$ of multiplication by 7. Then $s(d) \equiv 0(7)$ if and only if $E^d(\mathbb{Q})$ is infinite or $(\mathbf{W}^d)_7 \neq 0$.*

In particular, in the few cases below in which $s(d) = \pm 7$, we know that $E^d(\mathbb{Q})$ is finite, so $\mathbf{W}^d$ has nontrivial 7-torsion. Thus the order of $\mathbf{W}^d$ is at least 49.

TABLE I

$s(d)$

$d \equiv 1(4)$

0	53	57	149	193	197	201	237	373	381	437
	453	465	493	541	597	645	681	685	689	741
	745	849	885	913	957	989	1005	1045	1101	1149
	1165	1177	1229	1397	1401	1441	1469	1493	1509	1633
	1653	1685	1689	1713	1761	1781	1789	1829	1877	1909
1	1	5	29	33	37	69	97	101	109	137
	205	253	281	341	345	397	429	473	573	601
	617	661	717	733	737	769	773	781	797	865
	869	897	1069	1173	1181	1205	1213	1221	1261	1285
	1297	1349	1385	1585	1605	1657	1661	1693	1733	1765
	1797	1817	1861	1885	1945	1985	1997			
−1	13	17	41	61	65	85	145	165	173	181
	213	221	229	241	293	313	321	337	365	377
	461	517	545	565	569	613	641	649	653	701
	709	713	757	761	789	857	881	937	941	965
	1033	1061	1073	1077	1081	1129	1133	1157	1241	1293
	1333	1345	1353	1373	1381	1517	1541	1601	1609	1621
	1649	1705	1745	1749	1921	1977				
2	185	209	249	277	285	309	317	393	421	457
	481	489	629	633	705	809	813	821	901	1009
	1117	1121	1185	1189	1389	1417	1529	1537	1545	1569
	1581	1801	1837	1853	1901	1933	1961	1965	1969	
−2	93	113	129	141	417	501	557	589	817	893
	953	969	1209	1245	1265	1289	1437	1549	1597	1677
	1709	1769	1893	1905	1957					
3	73	157	233	349	389	409	433	521	673	853
	905	977	985	1065	1109	1153	1301	1313	1357	1429
	1473	1565	1669	1721	1793					
−3	89	265	269	305	401	445	485	505	509	533
	537	561	677	785	793	877	949	1041	1093	1201
	1217	1273	1329	1405	1433	1453	1501	1513	1637	1717
	1777	1865	1913	1937	1949					
4	449	669	921	1137	1257	1409	1497	1833		
−4	177	753	993	1317	1461	1481	1577	1641	1821	1929
5	257	1013	1037	1049	1097	1105	1237	1321	1361	1553
	1613	1697	1741							
−5	353	577	593	697	829	997	1145	1249	1277	1973
6	933	1857	1873							
−6	1457	1941								
7	929	1993								
−7	1021	1193	1465	1489	1753	1889				

TABLE I (*continued*)

$d \equiv 2, 3(4)$

0	10	11	43	47	62	66	79	122	134	138
	142	155	159	167	186	206	222	226	299	310
	311	319	347	354	358	370	382	383	398	407
	411	426	447	470	474	498	506	526	527	547
	591	598	607	642	699	727	755	786	831	843
	851	871	895	902	923	926	935	951	982	1034
	1055	1063	1119	1122	1158	1214	1219	1243	1262	1271
	1294	1366	1367	1371	1378	1391	1419	1443	1471	1479
	1518	1546	1555	1579	1583	1591	1595	1598	1606	1651
	1654	1658	1667	1686	1698	1702	1707	1739	1763	1766
	1767	1770	1786	1795	1814	1831	1851	1870	1887	1906
	1966	1999								
1	3	15	23	30	34	39	55	59	78	87
	102	118	127	130	151	178	187	195	219	227
	239	251	255	258	278	290	295	298	307	326
	355	359	366	390	391	418	431	443	451	466
	478	482	487	491	514	530	534	554	563	582
	626	627	635	638	646	662	683	690	695	723
	743	746	767	771	778	779	782	807	815	842
	899	911	934	967	978	1027	1042	1047	1082	1086
	1095	1114	1118	1131	1135	1139	1147	1159	1171	1182
	1202	1226	1247	1258	1282	1286	1303	1326	1374	1394
	1402	1403	1418	1427	1430	1455	1459	1478	1486	1514
	1515	1542	1562	1563	1586	1614	1634	1635	1643	1655
	1718	1735	1798	1802	1811	1830	1843	1858	1871	1886
	1894	1903	1910	1914	1954	1970	1986	1991		
−1	2	6	19	22	38	46	51	58	67	74
	83	86	95	106	107	110	111	115	123	139
	143	146	183	194	211	215	218	230	246	247
	254	267	274	283	286	303	318	327	330	339
	395	402	430	435	471	494	502	551	559	562
	583	590	610	615	634	655	667	674	678	687
	691	694	703	706	710	754	758	759	787	795
	802	803	814	827	830	838	858	859	907	915
	942	943	946	955	974	986	1003	1011	1023	1038
	1079	1110	1111	1126	1142	1167	1186	1187	1191	1199
	1230	1234	1235	1238	1254	1270	1291	1299	1306	1310
	1311	1342	1347	1363	1439	1462	1483	1502	1527	1531
	1535	1551	1558	1615	1627	1630	1679	1691	1711	1730
	1758	1759	1762	1803	1810	1822	1826	1839	1874	1902
	1943	1955	1983	1987						
2	26	94	103	114	158	163	170	174	199	235
	314	331	335	362	367	379	386	403	410	422
	439	442	458	479	538	570	579	611	618	631
	670	731	734	822	874	878	886	898	922	983
	998	1006	1007	1018	1030	1031	1054	1066	1151	1178

TABLE I (*continued*)

	1194	1195	1203	1207	1298	1319	1399	1410	1434	1447
	1454	1490	1495	1506	1507	1543	1590	1594	1607	1618
	1623	1626	1671	1695	1726	1742	1774	1838	1846	1927
	1947	1951	1982							
−2	31	71	191	214	223	263	271	282	334	346
	374	446	503	515	535	555	571	599	654	659
	682	698	715	739	762	766	794	799	823	835
	839	870	890	914	919	930	947	962	970	979
	991	995	1067	1070	1074	1102	1130	1146	1166	1198
	1263	1279	1283	1315	1334	1338	1339	1343	1355	1362
	1370	1406	1438	1474	1482	1487	1510	1523	1559	1578
	1639	1646	1670	1738	1747	1751	1790	1819	1823	1842
	1866	1898	1915	1923	1930	1938	1978			
3	131	166	179	190	262	323	415	519	543	566
	606	619	643	663	671	751	790	811	879	883
	894	939	1019	1051	1059	1087	1090	1091	1094	1103
	1123	1138	1163	1259	1266	1307	1318	1382	1390	1426
	1534	1570	1574	1619	1663	1703	1723	1727	1779	1794
	1807	1907	1919	1958	1959	1963				
−3	82	291	302	394	419	438	454	467	499	510
	523	614	718	818	862	866	971	1010	1046	1174
	1290	1335	1346	1387	1415	1423	1446	1522	1599	1662
	1699	1714	1867	1878	1895	1942				
4	622	719	730	806	906	1002	1039	1115	1222	1322
	1879									
−4	202	463	586	834	863	887	958	1327	1398	1451
	1466	1511	1567	1678	1787	1847	1882	1891	1990	1994
5	1227	1411	1642							
−5	587	1154	1255	1383	1499	1538	1731	1931	1934	1979
6	542	1223	1354	1706	1835					
−6	647	1231								
7	1622	1754								
−7	1571									
8	1783									

REFERENCES

1. B. J. BIRCH AND W. KUYK (Eds.), Modular functions of one variable IV. *in* "Lecture Notes in Math.," Vol. 476, Springer–Verlag, Berlin, 1975.
2. H. BRANDT AND O. INTRAU, Tabellen reduzierter positiver ternärer quadratischer Formen, *Abh. Sächs. Akad. Wiss. Leipzig Math.-Natur. Kl.* **45**, No. 4 (1958).

3. J. P. BUHLER, Icosahedral galois representations, *in* "Lecture Notes in Math.," Vol. 654, Springer–Verlag, Berlin, 1978.
4. J. W. S. CASSELS, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.
5. J. COATES AND A. WILES, On the conjecture of Birch and Swinnerton–Dyer, *Invent. Math.* **39** (1977), 223–251.
6. H. COHEN AND J. OESTERLE, Dimensions des espaces de formes modulaires, *in* "Lecture Notes in Math.," Vol. 627, pp. 69–78, Springer–Verlag, Berlin, 1977.
7. A. FRÖHLICH (Ed.), "Algebraic Number Fields," Academic Press, London, 1977.
8. B. H. GROSS, Arithmetic on elliptic curves with complex multiplication, *in* "Lecture Notes in Math.," Vol. 776, Springer–Verlag, Berlin, 1980.
9. T. HADANO, Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor, *Proc. Japan Acad.* **51** (1975), 92–95.
10. N. KOBLITZ, "Introduction to Elliptic Curves and Modular Forms," Springer–Verlag, New York, 1984.
11. N. KOBLITZ (Ed.), "Number Theory Related to Fermat's Last Theorem," Birkhäuser, Boston, MA., 1982.
12. J. L. LEHMAN, "An Application of the Shimura Correspondence to the Modular Curve $X_0(49)$," Thesis, University of Virginia, January 1986.
13. B. SCHOENEBERG, "Elliptic Modular Functions: An Introduction," Springer–Verlag, New York, 1974.
14. R. SCHULZE-PILLOT, Thetareihen positiv definiter quadratischer Formen, *Invent. Math.* **75** (1984), 283–299.
15. J.-P. SERRE AND H. M. STARK, Moduar forms of weight $\frac{1}{2}$, "Lecture Notes in Math.," Vol. 627, pp. 27–67, Springer–Verlag, Berlin, 1977.
16. G. SHIMURA, On modular forms of half-integral weight, *Ann. of Math.* **97** (1973), 440–481.
17. G. STEVENS, "Arithmetic on Modular Curves," Birkhäuser, Boston, MA., 1982.
18. J. T. TATE, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.
19. J. B. TUNNELL, A classical Diophantine problem and modular forms of weight $\frac{3}{2}$, *Invent. Math.* **72** (1983), 323–334.
20. J.-L. WALDSPURGER, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* **60** (1981), 375–484.